UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/711,169 | 11/13/2000 | James Monroe Clark | 0918.0037C | 6625 |

7590 10/19/2004

Epstein Edell Shapiro & Finnan LLC
1901 Research Boulevard
Suite 400
Rockville, MD 20850-3164

| EXAMINER | |
|---|---|
| SIMITOSKI, MICHAEL J | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2134 | |

DATE MAILED: 10/19/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/711,169 | CLARK, JAMES MONROE | |
| | Examiner | Art Unit | |
| | Michael J Simitoski | 2134 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *07 September 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,7,8,11-14,16,17,19-25,29,30,33-36,38,39,42 and 44* is/are rejected.

7)☒ Claim(s) *5,6,9,10,15,18,26-28,31,32,37,40,41 and 43* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 November 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

1. The response of 9/7/2004 was received and considered.

2. Claims 1-44 are pending.

3. The examiner notes that the response filed 9/7/2004 refers to application 09/711,156. However, the transmittal for the response refers to the instant application, and therefore the response is understood to refer to the instant application, 09/711,169.

### *Response to Arguments*

4. Regarding the rejections under 35 U.S.C. §112 of claims 3 and 4, in light of applicant's explanation and clarification of the term "random" as it is used in the claims, the rejections are withdrawn.

5. Applicant's arguments filed 9/7/2004 have been fully considered but they are not persuasive.

Regarding applicant's arguments (page 4 of REMARKS, ¶3), applicant asserts that Ritter does not teach conditionally changing the value of individual symbols of each data element in the input block, but rather walks through byte-by-byte. Applicant is directed to Ritter, page 4, ¶2-7, where Ritter discloses exchanging a byte with a partner byte (specifically, ¶2). The individual symbols, in this case bits making up the bytes, are changed during this process and therefore, the Ritter reference reads on the argued limitation.

### *Claim Rejections - 35 USC § 112*

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 42 & 44 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The claim merely presents intended statistical properties of an output, rather than apparatus limitations or active method steps.

***Claim Rejections - 35 USC § 102***

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claims 1, 2, 11 are rejected under 35 U.S.C. 102(b) as being anticipated by "Transposition Cipher with Pseudo-Random Shuffling: The Dynamic Transposition Combiner" by Ritter.

Regarding claims 1, 11, Ritter discloses generating an input block of data elements/bytes/characters (page 4, ¶2 & ¶5), where each data element occupies a particular position in the input block (page 2, ¶3), each data element being represented by plural symbols/bits (page 4, ¶2-3 (byte=plurality of bits)), and for each data element/byte/character in the input block, conditionally changing the value of the individual symbols/bits of the data element/byte/character (page 4, ¶2) in accordance with random data/random number generator (page 4, ¶2) to form an output data element in a corresponding position in an output block of data elements (page 4, ¶2), the output data element being one of the data elements in the input block

(page 4, ¶2 & ¶7), wherein each data element is mapped from a position in the input block to a position in the output block, such that the output block of data elements is a random permutation of the input block of data elements (page 4, ¶2 & ¶7).

Regarding claim 2, Ritter discloses retrieving a random symbol/number and determining a value of a corresponding symbol/byte represented in bits of the output data element as a function of the symbol/bytes represented in bits of the data element/byte/character and the random symbol/number (page 4, ¶2).

***Claim Rejections - 35 USC § 103***

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 3, 14 & 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ritter.

Regarding claim 3, Ritter, as best understood, does not explicitly disclose a system where the output of the permutation is the exclusive-OR of the symbol of the data element and the random symbol. However, Ritter explains that to ensure good performance, the input data can be exclusive-OR'd with a pseudo-random stream (page 4, ¶5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to exclusive-OR the input data with a pseudo-random stream. One of ordinary skill in the art would have been motivated to perform such a modification to ensure good performance, as taught by Ritter (page 4, ¶5).

Regarding claim 14, Ritter does not specifically place the constraint that each data element/character only occur once in the input block. However, Ritter teaches that a character or byte transposition combiner can provide good performance only when given a block containing different values (page 4, ¶5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to allow each element in the input block to occur only once. One of ordinary skill in the art would have been motivated to perform such a modification to guarantee good performance, as taught by Ritter (page 4, ¶5).

Regarding claim 16, Ritter does not specifically disclose $2^N$ data elements where N is a positive integer. However, Ritter teaches that 64 elements in a block would have a very low probability of correct random decipherment (page 3, ¶2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use 64 $\left(= 2^6\right)$ data elements in a block. One of ordinary skill in the art would have been motivated to perform such a modification to obtain a very low probability of correct random decipherment, as taught by Ritter (page 3, ¶2).

12. Claims 12 & 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ritter, as applied to claim 1 above, in view of U.S. Patent 4,476,566 to Dent. Ritter does not disclose inputting a sequence of incrementing numbers or transmission frequencies in a frequency-hopping communication system, and the output being a hop code sequence. However, Dent teaches that some RF communications systems employ frequency hopping where the carrier frequency of each radio is randomly changed to provide some immunity to jamming (col. 1, lines 14-60). A clock/periodic signal controls a counter (Fig. 2) that identifies the channels/frequencies (col. 1, lines 63-69). The Dent invention has the benefit of increased

number of radios that can operate (col. 1, lines 54-60). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to input a sequence of increasing numbers, and use the random permutation generator disclosed by Ritter to select frequencies in a frequency-hopping communication system where the output sequence is a hop code sequence. One of ordinary skill in the art would have been motivated to perform such a modification to increase the number of radios that can operate (col. 1, lines 14-69 & Fig. 2).

13. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ritter, as applied to claim 1, in view of U.S. Patent 6,400,824 to Mansoorian et al. (Mansoorian). Ritter does not disclose forming a truncated permutation of only a subset of the data elements. However, Mansoorian teaches that in DES, a well-known encryption scheme, operations such as permutations act on subsets of the input data in different rounds (col. 2, lines 1-20). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to form a truncated permutation of only a subset of the data elements. One of ordinary skill in the art would have been motivated to perform such a modification to employ the permutation system in the DES encryption scheme, as taught by Mansoorian (col. 2, lines 1-20).

14. Claims 4, 19, 20, 22-25, 33, 36 & 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ritter in view of U.S. Patent 4,876,659 to Devereux et al. (Devereux).

Regarding claim 4, Ritter does not disclose an address. However, Devereux teaches a pseudo-random code generator that stores random codes/code bits in a memory to be outputted partly under the control of a counter (col. 2, lines 25-43). The system has the benefits of significant reduction in the size and power consumption (col. 2, lines 25-43). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was

made to include a random code memory. One of ordinary skill in the art would have been motivated to perform such a modification to store random codes with the benefits of reduced size and power consumption, as taught by Devereux (col. 2, lines 25-43). Ritter discloses data elements (containing bits 1 and 0), and a memory location is addressable by 1's and 0's and therefore the address must comprise symbols from at least one of the data element and the output data element.

Regarding claims 19, 22 & 33, Ritter discloses a method, as described in claim 1 above, but lacks explicitly an input device configured to supply the blocks of data elements, a random code memory device for storing random data, and a permutation logic unit to perform the functions substantially equivalent to those of part (b) in claim 1. However, Devereux teaches a pseudo-random code generator that stores random codes/code bits in a memory to be outputted partly under the control of a counter (col. 2, lines 25-43). The system has the benefits of significant reduction in the size and power consumption (col. 2, lines 25-43). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a random code memory. One of ordinary skill in the art would have been motivated to perform such a modification to store random codes with the benefits of reduced size and power consumption, as taught by Devereux (col. 2, lines 25-43). Regarding the input device supplying blocks of data elements and permutation logic unit, while Ritter does not explicitly disclose these physical devices, the examiner takes Official Notice that input devices (such as data buffers or external sources) and using logic (processors) are old and well established techniques in the art of computer data processing as a method of receiving binary data and performing computations on the data. Therefore, it would have been obvious to one having

ordinary skill in the art at the time the invention was made to include an input device. One of ordinary skill in the art would have been motivated to perform such a modification to physically enable the permutation process, taught by Ritter, on a computing device. This advantage is well known to those skilled in the art.

Regarding claim 20, while Ritter does not explicitly disclose an output register, the examiner takes Official Notice that output registers are old and well established in the art of computer architecture as a method of storing outputted data from a computing device. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include an output register to receive each output data element generated by the permutation logic unit. One of ordinary skill in the art would have been motivated to perform such a modification to store the results of the permutation logic unit. This advantage is well known to those skilled in the art.

Regarding claim 23, Ritter, as modified above, discloses retrieving a random symbol/random number (Ritter, page 2, ¶4) from the random code memory device (Devereux, Figs. 2a & 2b) and determines the value of a corresponding symbol of the output data element as a function of the symbol of the data element and the random symbol (Ritter, page 4, ¶2).

Regarding claim 24, Ritter, does not explicitly disclose a system where the output of the permutation is the exclusive-OR of the symbol of the data element and the random symbol. However, Ritter explains that to ensure good performance, the input data can be exclusive-OR'd with a pseudo-random stream (page 4, ¶5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to exclusive-OR the input data with a

pseudo-random stream. One of ordinary skill in the art would have been motivated to perform such a modification to ensure good performance, as taught by Ritter (page 4, ¶5).

Regarding claim 25, Ritter, as modified above, discloses a memory (col. 2, lines 25-43). As the input and output data elements are collections of bits (1 or 0), the address comprises symbols (bits) from at least one of the data element and the output data element.

Regarding claim 36, Ritter does not specifically place the constraint that each data element/character only occur once in the input block. However, Ritter teaches that a character or byte transposition combiner can provide good performance only when given a block containing different values (page 4, ¶5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to allow each element in the input block to occur only once. One of ordinary skill in the art would have been motivated to perform such a modification to guarantee good performance, as taught by Ritter (page 4, ¶5).

Regarding claim 38, Ritter does not specifically disclose $2^N$ data elements where N is a positive integer. However, Ritter teaches that 64 elements in a block would have a very low probability of correct random decipherment (page 3, ¶2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use 64 $\left(=2^6\right)$ data elements in a block. One of ordinary skill in the art would have been motivated to perform such a modification to obtain a very low probability of correct random decipherment, as taught by Ritter (page 3, ¶2).

15. Claims 7, 8, 21, 29, 30, 34 & 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ritter in view of Devereux, as applied to claim 19 above, in further view of U.S. Patent 4,476,566 to Dent.

Regarding claims 21, 34 & 35, Ritter does not disclose a counter that periodically supplied an incremented number in response to a periodic signal. However, Dent teaches that some RF communications systems employ frequency hopping where the carrier frequency of each radio is randomly changed to provide some immunity to jamming (col. 1, lines 14-60). A clock/periodic signal controls a counter (Fig. 2) that identifies the channels/frequencies (col. 1, lines 63-69). The Dent invention has the benefit of increased number of radios that can operate (col. 1, lines 54-60). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the dynamic transposition cipher using random data as the random generator for frequency hopping, where a counter periodically supplies an incremented number in response to a periodic signal. One of ordinary skill in the art would have been motivated to perform such a modification to increase the number of radios that can operate, as taught by Dent (col. 1, lines 14-69 & Fig. 2).

Regarding claims 7, 8, 29 & 30, Ritter, as modified above, lacks repeatedly performing the supplying input and forming output functions and lacks storing altered random data. However, Dent teaches that some RF communications systems employ frequency hopping where the carrier frequency of each radio is randomly changed to provide some immunity to jamming (col. 1, lines 14-60). A clock/periodic signal controls a counter (Fig. 2) that identifies the channels/frequencies (col. 1, lines 63-69). The Dent invention has the benefit of increased number of radios that can operate (col. 1, lines 54-60). Further, Ritter discloses that the purpose of applying a continuing pseudo-random sequence is to guarantee that the blocks will always be permuted differently (page 2, ¶4). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the dynamic transposition cipher using

random data as the random generator for frequency hopping. One of ordinary skill in the art would have been motivated to perform such a modification to increase the number of radios that can operate, as taught by Dent (col. 1, lines 14-69 & Fig. 2). It would have been further obvious to one having ordinary skill in the art at the time the invention was made to periodically store altered random data. One of ordinary skill in the art would have been motivated to perform such a modification to ensure that all blocks are likely to be permuted differently, as taught by Ritter (page 2, ¶4). Lastly, as modified by Dent, the frequency hopping system that employs the pseudo-random function is a continuous system (clock) (col. 1, line 63 – col. 2, line 43 & Fig. 2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to repeat the steps of Ritter's pseudo-random permutation generator. One of ordinary skill in the art would have been motivated to perform such a modification to provide continuously random data, as taught by Dent (col. 1, line 63 – col. 2, line 43 & Fig. 2).

16. Claim 39 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ritter in view of Devereux, as applied to claim 19, in view of U.S. Patent 6,400,824 to Mansoorian et al. (Mansoorian). Ritter does not disclose forming a truncated permutation of only a subset of the data elements. However, Mansoorian teaches that in DES, a well-known encryption scheme, operations such as permutations act on subsets of the input data in different rounds (col. 2, lines 1-20). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to form a truncated permutation of only a subset of the data elements. One of ordinary skill in the art would have been motivated to perform such a modification to employ the permutation system in the DES encryption scheme, as taught by Mansoorian (col. 2, lines 1-20).

### *Allowable Subject Matter*

17. Claims 5-6, 9-10, 15, 18, 26-28, 31-32, 37, 40-41 & 43 are objected to as being dependent upon a rejected base claim, but are believed to be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

### *Conclusion*

18. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (703) 305-8191. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (703) 308-4789.

**Any response to this action should be mailed to:**

Commissioner of Patents and Trademarks
Washington, DC 20231

**Or faxed to:**

(703)746-7239 (for formal communications intended for entry)

**Or:**

(703)746-7240 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-9000.

*NOTE: After October 19, 2004, Michael Simitoski can be reached at (571) 272-3841, Greg Morse can be reached at (571) 272-3838 and general inquiries can be directed to (571) 272-2100.*

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
October 12, 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100